Cost and Schedule

BAE SYSTEMS

The Overlooked Hazard

By: Ronald Stroup
FAA Safety and Certification Lead

Warren Naylor
BAE SYSTEMS System Safety Manager

The Problem

BAE SYSTEMS

- Failure to recognize and address cost & schedule as causal factors that could result in avoidable catastrophic events.

The Environment

- Absolutely no one intentionally builds an unsafe system!
- However, systems are routinely built that are not as safe as they reasonably should be.
  - Some of these systems are built by qualified systems engineers, professional safety professionals, and are managed by program managers, which employ the latest software and development methodologies, yet the end product routinely misses expectations.

The Environment (cont'd)

- Schedules for programs have become increasingly more aggressive, contracts have become increasingly more restrictive, and start dates are continually pushed back without corresponding relief on the back end, resulting in extremely compressed schedules.
- Schedule overruns and their accompanying cost overruns have become the rule rather than the exception.
- How does this happen?

Paper Intent

- The intent of this paper is not to assign blame, it is to assist the development community in developing safer and ultimately better products by identifying a deficiency that we believe most recognize but feel powerless to correct.

Decisions Under Duress

- Shortcuts are taken when budgets and schedules become tight.
- Decisions to mitigate cost and schedule overages are usually comprised of:
  - Reductions in developmental testing
  - Reductions in integration testing
  - Shortcuts on standard development processes (e.g. reviews)
  - Reduction in system functionality
  - Reduction in training

Case History 1 – V-22 Osprey

BAE SYSTEMS

"To save time and money, … omitted tests of the V-22 Osprey that would have provided additional data on rapid descents that contributed to a crash that killed 19 Marines in April, according to a new report by the General Accounting Office."

Flaherty and Ricks., The Washington Post. Front Page `9 February 2001.

Osprey Lessons Learned

- Unfortunately, as evidenced with the Osprey program, systems testing falls at the end of the development process regardless of the development model used, thereby, becoming a casualty of schedule and cost overruns.
- Unfortunately, the Osprey Program was so over budget and schedule and under severe scrutiny by both the media and Congress, that the maintenance and flight availability data were allegedly falsified to ensure the program's ultimate survival.

Case History 2 - Advanced Automation System (AAS)

BAE SYSTEMS

- The Federal Aviation Administration's AAS program was a challenging program to replace the computer hardware and software, including controller workstations, in en-route, terminal, and tower air traffic control facilities in hopes of providing new automated capabilities to accommodate increases in air traffic.

Case History 2 - AAS) (cont'd)

- The AAS software was ranked among the most complex software development projects in the world and was expected to operate in a real-time environment in which hundreds of functions must be executed within seconds and was expected to be fault tolerant.

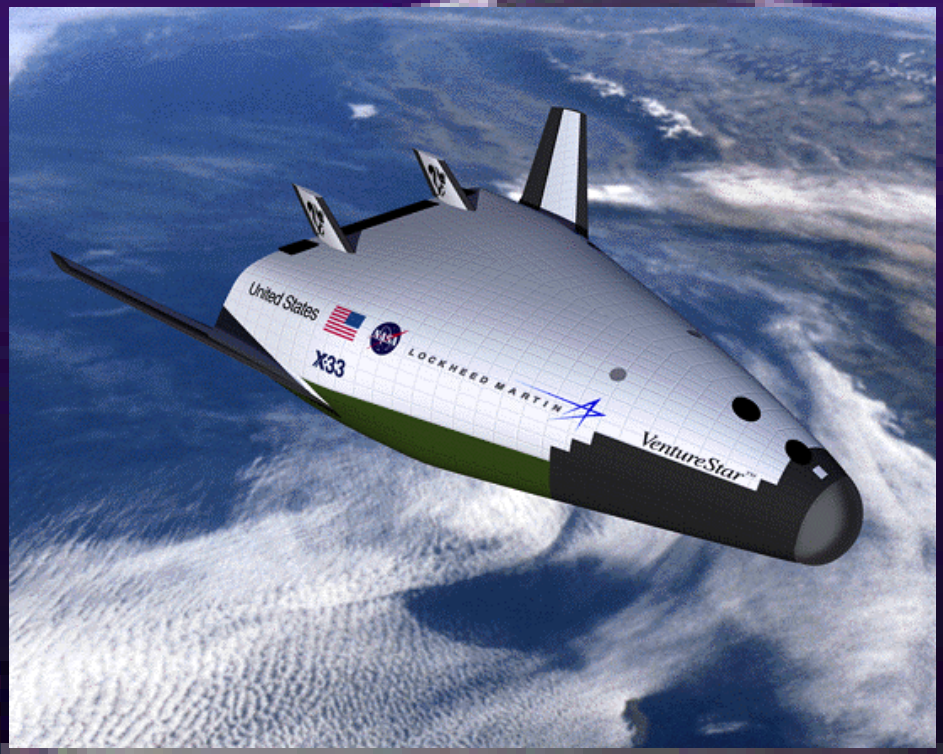
AAS Lessons Learned

- The shot gun approach to developing a system of the complexity of AAS proved ineffective. The program failed to meet their defined objectives; specifically (ref. 2)
  - Failed to meet reliability objective
  - Design contained unwanted features
  - Current state of technology could not support the design
  - Failure to achieve defined testing objectives
  - System as a whole was never deployed.

2 Glass, R., Software Runaways. Prentice Hall PTR, 1998

Case History 3 – VentureStar

BAE SYSTEMS



- Former Astronaut Carl Mead acknowledged in the Washington Post article “from the outside the project looked like all bad news, but it felt normal.”

VentureStar Lessons Learned

BAE SYSTEMS

- Conflicting requirements imposed by scientific, political, military, and commercial interests can adversely affect cost and schedule
- Design leapt ahead of economic and technical realities
  - –Maintaining the bleeding edge of technology is cost, schedule, and mission prohibitive
  - –Let others debug the new technologies

Mitigating Strategies

- Those strategies that can help alleviate cost and schedule overruns are:
  - Consistent goals among the stakeholders
  - Coordination among stakeholders.
  - Proper contract application
  - Evolutionary life cycle

Consistent Goals Among Stakeholders

- In many organizations the role of safety engineering is separate from the development team. This separation can often result in inconsistent goals.
- The goal of the program manager is to fulfill the requirements pertaining to the design, development, production and delivery of the system in an effective, efficient, and timely manner. In many instances, cost and schedule become the driving factor in meeting the goal (ref. 5).
-

5 Blanchard and Fabrycky., Systems Engineering and Analysis, 3rd Edition, 1998, Prentice-Hall Inc.

Consistent Goals Among Stakeholders (cont'd)

- Management's attempts to meet strict schedules by reducing functionality and safety constraints, although well intentioned, are often misguided, as the PM is often inadvertently and sometimes advertently not informed of the inherent risks these shortcuts induce on the project.
- Over time the safety margin is eroded and there are no up-to-date data on the current or proposed residual risk of the deleted functionality.
- Programmatic risk is the driver in this situation with safety risk often being overlooked or set aside.

Coordination Among Stakeholders

- Highly complex systems require coordination between stakeholders to ensure all of the components come together into a safe and effective system. The coordinating body should also ensure the necessary evidence of completion is obtained before additional steps are undertaken
  - The FAA is proposing the development of a Coordinated Operational Approval Process (COAP) to perform this function
  - In the US Navy the WSESRB/SSSTRP fulfills this need

Proper Contract Application

- The type of contract (fixed price, cost plus, incentive fee agreement with cost ceiling, etc.) can play a large role in the effectiveness or ineffectiveness of a program's ability to ensure goals are met.
- The majority of contracts make payments based on time spent and materials used rather than timeliness and efficiency.
- Until the payments are directly linked to the completion of deliverables, there is no incentive for the contractor to control costs or use labor efficiently.

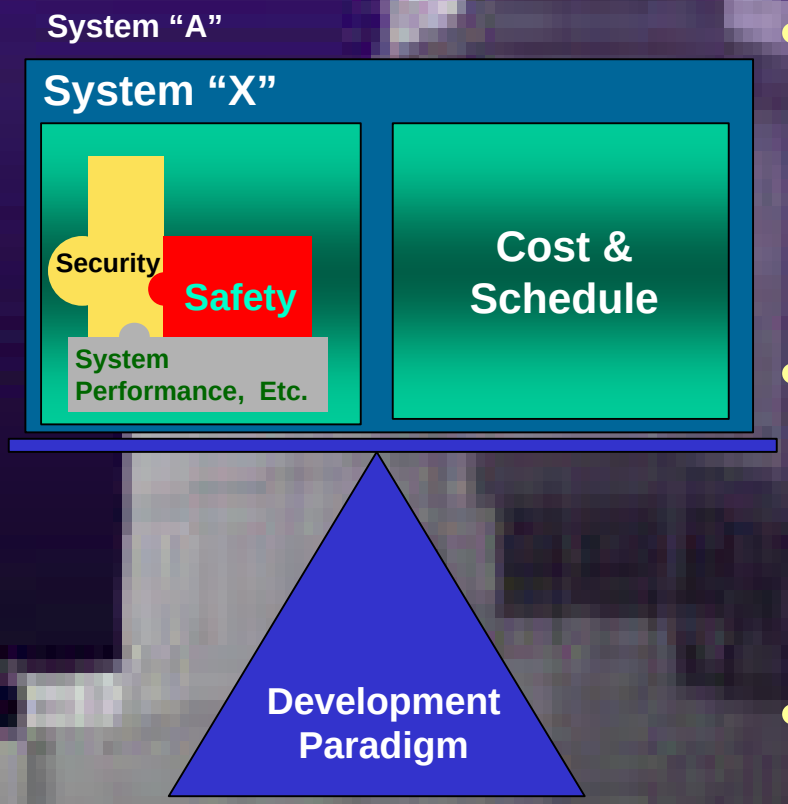
Evolutionary Life Cycle

- Big-bang development is not an effective means to develop highly complex safety critical systems.
- The name of the game is “risk reduction,” which means it must be developed to an evolutionary life cycle process.
- Modernization of complex software-intensive systems must be evolutionary: develop a new system that performs today’s functions while maintaining expandability. Then add new or enhanced functionality. Build a little, test a little.
- The FAA’s Federal Acquisition Executive stated, “We need to be more risk averse. We’ve learned not to push the boundaries of science (ref. 7).”
-

7 Perry, T., In Search of the Future of Air Traffic Control. IEEE Spectrum, August 1997.

Safety's Role in the Cost & Schedule Paradigm

BAE SYSTEMS



- Safety can play a significant and sometimes contributory role in the cost and schedule paradigm.
- Safety's contribution can impact the cost and schedule both positively and negatively.
- The goal of any project should be to achieve a balance in terms of cost and safety.

How Can Safety Mitigate any Negative Impact on Cost & Schedule

- Safety must identify, assess, and report identified hazards as soon as possible in the development process to ensure they are properly and comprehensively mitigated.
- Failure to do so dooms a system to redesign and rework, resulting in a system that fails to meet its targeted and often even acceptable levels of safety and performance risk.
- A balance must be maintained between system safety, system performance, and all other contributory disciplines with cost and schedule

Safety Order of Precedence

1. Design for minimum risk.
2. Incorporate safety devices
3. Design warning devices
4. Develop procedures and training

Any Questions?

BAE SYSTEMS